AMENDMENTS TO CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

1. (Currently amended) An apparatus for performing a SubByte function of the Rijndael Block Cipher, comprising:

an S-box circuit including

an inverse transformation circuit having a lookup table and being configured and arranged to transform an input using a look-up table, wherein the look-up table is the multiplicative inverse in the finite field GF(2^8) having {00} mapped to itself, and the look-up table is implemented by a read-only memory (ROM);

a combinational logic circuit configured and arranged to perform an affine-all transformation that performs both an affine and inverse affine transformation in response to respective load patterns, wherein the combinatorial logic circuit implements the equations:

$$b'_0=[(b_0 \cdot p_0)\oplus(b_1 \cdot p_1)\oplus(b_2 \cdot p_2)\oplus(b_3 \cdot p_3)\oplus(b_4 \cdot p_4)\oplus(b_5 \cdot p_5)\oplus(b_6 \cdot p_6)\oplus(b_7 \cdot p_7)]\oplus v_0$$
$$b'_1=[(b_0 \cdot p_7)\oplus(b_1 \cdot p_0)\oplus(b_2 \cdot p_1)\oplus(b_3 \cdot p_2)\oplus(b_4 \cdot p_3)\oplus(b_5 \cdot p_4)\oplus(b_6 \cdot p_5)\oplus(b_7 \cdot p_6)]\oplus v_1$$
$$b'_2=[(b_0 \cdot p_6)\oplus(b_1 \cdot p_7)\oplus(b_2 \cdot p_0)\oplus(b_3 \cdot p_1)\oplus(b_4 \cdot p_2)\oplus(b_5 \cdot p_3)\oplus(b_6 \cdot p_4)\oplus(b_7 \cdot p_5)]\oplus v_2$$
$$b'_3=[(b_0 \cdot p_5)\oplus(b_1 \cdot p_6)\oplus(b_2 \cdot p_7)\oplus(b_3 \cdot p_0)\oplus(b_4 \cdot p_1)\oplus(b_5 \cdot p_2)\oplus(b_6 \cdot p_3)\oplus(b_7 \cdot p_4)]\oplus v_3$$
$$b'_4=[(b_0 \cdot p_4)\oplus(b_1 \cdot p_5)\oplus(b_2 \cdot p_6)\oplus(b_3 \cdot p_7)\oplus(b_4 \cdot p_0)\oplus(b_5 \cdot p_1)\oplus(b_6 \cdot p_2)\oplus(b_7 \cdot p_3)]\oplus v_4$$
$$b'_5=[(b_0 \cdot p_3)\oplus(b_1 \cdot p_4)\oplus(b_2 \cdot p_5)\oplus(b_3 \cdot p_6)\oplus(b_4 \cdot p_7)\oplus(b_5 \cdot p_0)\oplus(b_6 \cdot p_1)\oplus(b_7 \cdot p_2)]\oplus v_5$$
$$b'_6=[(b_0 \cdot p_2)\oplus(b_1 \cdot p_3)\oplus(b_2 \cdot p_4)\oplus(b_3 \cdot p_5)\oplus(b_4 \cdot p_6)\oplus(b_5 \cdot p_7)\oplus(b_6 \cdot p_0)\oplus(b_7 \cdot p_1)]\oplus v_6$$
$$b'_7=[(b_0 \cdot p_1)\oplus(b_1 \cdot p_2)\oplus(b_2 \cdot p_3)\oplus(b_3 \cdot p_4)\oplus(b_4 \cdot p_5)\oplus(b_5 \cdot p_6)\oplus(b_6 \cdot p_7)\oplus(b_7 \cdot p_0)]\oplus v_7$$

---

having $p = p_0p_1p_2p_3p_4p_5p_6p_7$ as a load pattern consisting of {10001111} for the affine transformation and {00100101} for the inverse affine transformation and having v as a load vector = $v_0v_1v_2v_3v_4v_5v_6v_7$ consisting of {11000110} for the affine transformation and {10100000} for the inverse affine transformation.

2-3. (Cancelled).

4. (Previously presented) An apparatus for encrypting and decrypting data, comprising:

a data processing module arranged to perform a byte substitution, wherein at least part

of said data processing module comprises:

a look-up table which is the multiplicative inverse in the finite field GF(2^8) having {00} mapped to itself, and the look-up table is implemented by a read-only memory (ROM),

a storage device for storing the look-up table, and

a circuit having shared logic that performs a single transform that accomplishes an affine and an inverse affine transformation, wherein the circuit having shared logic implements the equations:

$$b'_0=[(b_0 \cdot p_0)\oplus(b_1 \cdot p_1)\oplus(b_2 \cdot p_2)\oplus(b_3 \cdot p_3)\oplus(b_4 \cdot p_4)\oplus(b_5 \cdot p_5)\oplus(b_6 \cdot p_6)\oplus(b_7 \cdot p_7)]\oplus v_0$$
$$b'_1=[(b_0 \cdot p_7)\oplus(b_1 \cdot p_0)\oplus(b_2 \cdot p_1)\oplus(b_3 \cdot p_2)\oplus(b_4 \cdot p_3)\oplus(b_5 \cdot p_4)\oplus(b_6 \cdot p_5)\oplus(b_7 \cdot p_6)]\oplus v_1$$
$$b'_2=[(b_0 \cdot p_6)\oplus(b_1 \cdot p_7)\oplus(b_2 \cdot p_0)\oplus(b_3 \cdot p_1)\oplus(b_4 \cdot p_2)\oplus(b_5 \cdot p_3)\oplus(b_6 \cdot p_4)\oplus(b_7 \cdot p_5)]\oplus v_2$$
$$b'_3=[(b_0 \cdot p_5)\oplus(b_1 \cdot p_6)\oplus(b_2 \cdot p_7)\oplus(b_3 \cdot p_0)\oplus(b_4 \cdot p_1)\oplus(b_5 \cdot p_2)\oplus(b_6 \cdot p_3)\oplus(b_7 \cdot p_4)]\oplus v_3$$
$$b'_4=[(b_0 \cdot p_4)\oplus(b_1 \cdot p_5)\oplus(b_2 \cdot p_6)\oplus(b_3 \cdot p_7)\oplus(b_4 \cdot p_0)\oplus(b_5 \cdot p_1)\oplus(b_6 \cdot p_2)\oplus(b_7 \cdot p_3)]\oplus v_4$$
$$b'_5=[(b_0 \cdot p_3)\oplus(b_1 \cdot p_4)\oplus(b_2 \cdot p_5)\oplus(b_3 \cdot p_6)\oplus(b_4 \cdot p_7)\oplus(b_5 \cdot p_0)\oplus(b_6 \cdot p_1)\oplus(b_7 \cdot p_2)]\oplus v_5$$
$$b'_6=[(b_0 \cdot p_2)\oplus(b_1 \cdot p_3)\oplus(b_2 \cdot p_4)\oplus(b_3 \cdot p_5)\oplus(b_4 \cdot p_6)\oplus(b_5 \cdot p_7)\oplus(b_6 \cdot p_0)\oplus(b_7 \cdot p_1)]\oplus v_6$$
$$b'_7=[(b_0 \cdot p_1)\oplus(b_1 \cdot p_2)\oplus(b_2 \cdot p_3)\oplus(b_3 \cdot p_4)\oplus(b_4 \cdot p_5)\oplus(b_5 \cdot p_6)\oplus(b_6 \cdot p_7)\oplus(b_7 \cdot p_0)]\oplus v_7$$

---

having $p = p_0p_1p_2p_3p_4p_5p_6p_7$ as a load pattern consisting of {10001111} for the affine transformation and {00100101} for the inverse affine transformation and having v as a load vector = $v_0v_1v_2v_3v_4v_5v_6v_7$ consisting of {11000110} for the affine transformation and {10100000} for the inverse affine transformation.

5-7. (Cancelled) The apparatus as claimed in claim 4 wherein said look-up table is a multiplicative inverse of the finite field GF(2^8).

8. (Original) The apparatus as claimed in claim 4, wherein the apparatus comprises a plurality of instances of a data processing module arranged in a data processing pipeline.

9. (Original) The apparatus as claimed in claim 4, wherein the apparatus is arranged to perform encryption or decryption in accordance with the Rijndael Block Cipher, and wherein the data processing module is arranged to implement a Rijndael round.

10. (Original) An apparatus as claimed in claim 9, wherein the data processing module is arranged to implement the SubByte transformation of the Rijndael round using the lookup table composed with the affine transformation for encryption and the inverse affine

transformation for decryption.

11. (Previously presented) The apparatus as claimed in claim 10, wherein said look-up table is implemented by means of a read only memory (ROM).

12. (Currently amended) A apparatus for performing a SubByte function of a round of the Rijndael Block Cipher, comprising an S-box constructed by composing,

means for obtaining the multiplicative inverse in the finite field $GF(2^8)$, and

means for performing an affine-all transformation consisting of an affine and inverse affine transformation as a single affine transformation, wherein the means for performing implements the equations:

$$b'_0=[(b_0 \cdot p_0)\oplus(b_1 \cdot p_1)\oplus(b_2 \cdot p_2)\oplus(b_3 \cdot p_3)\oplus(b_4 \cdot p_4)\oplus(b_5 \cdot p_5)\oplus(b_6 \cdot p_6)\oplus(b_7 \cdot p_7)]\oplus v_0$$
$$b'_1=[(b_0 \cdot p_7)\oplus(b_1 \cdot p_0)\oplus(b_2 \cdot p_1)\oplus(b_3 \cdot p_2)\oplus(b_4 \cdot p_3)\oplus(b_5 \cdot p_4)\oplus(b_6 \cdot p_5)\oplus(b_7 \cdot p_6)]\oplus v_1$$
$$b'_2=[(b_0 \cdot p_6)\oplus(b_1 \cdot p_7)\oplus(b_2 \cdot p_0)\oplus(b_3 \cdot p_1)\oplus(b_4 \cdot p_2)\oplus(b_5 \cdot p_3)\oplus(b_6 \cdot p_4)\oplus(b_7 \cdot p_5)]\oplus v_2$$
$$b'_3=[(b_0 \cdot p_5)\oplus(b_1 \cdot p_6)\oplus(b_2 \cdot p_7)\oplus(b_3 \cdot p_0)\oplus(b_4 \cdot p_1)\oplus(b_5 \cdot p_2)\oplus(b_6 \cdot p_3)\oplus(b_7 \cdot p_4)]\oplus v_3$$
$$b'_4=[(b_0 \cdot p_4)\oplus(b_1 \cdot p_5)\oplus(b_2 \cdot p_6)\oplus(b_3 \cdot p_7)\oplus(b_4 \cdot p_0)\oplus(b_5 \cdot p_1)\oplus(b_6 \cdot p_2)\oplus(b_7 \cdot p_3)]\oplus v_4$$
$$b'_5=[(b_0 \cdot p_3)\oplus(b_1 \cdot p_4)\oplus(b_2 \cdot p_5)\oplus(b_3 \cdot p_6)\oplus(b_4 \cdot p_7)\oplus(b_5 \cdot p_0)\oplus(b_6 \cdot p_1)\oplus(b_7 \cdot p_2)]\oplus v_5$$
$$b'_6=[(b_0 \cdot p_2)\oplus(b_1 \cdot p_3)\oplus(b_2 \cdot p_4)\oplus(b_3 \cdot p_5)\oplus(b_4 \cdot p_6)\oplus(b_5 \cdot p_7)\oplus(b_6 \cdot p_0)\oplus(b_7 \cdot p_1)]\oplus v_6$$
$$b'_7=[(b_0 \cdot p_1)\oplus(b_1 \cdot p_2)\oplus(b_2 \cdot p_3)\oplus(b_3 \cdot p_4)\oplus(b_4 \cdot p_5)\oplus(b_5 \cdot p_6)\oplus(b_6 \cdot p_7)\oplus(b_7 \cdot p_0)]\oplus v_7$$

---

having $p = p_0p_1p_2p_3p_4p_5p_6p_7$ as a load pattern consisting of {10001111} for the affine transformation and {00100101} for the inverse affine transformation and having v as a load vector = $v_0v_1v_2v_3v_4v_5v_6v_7$ consisting of {11000110} for the affine transformation and {10100000} for the inverse affine transformation.

13. (Previously presented) The apparatus as claimed in claim 12, wherein said means for obtaining the multiplicative inverse is a look-up table, and said means for performing the affine-all transformation is a combinational logic circuit.

14. (Currently amended) A method for performing a SubByte function of a Rijndael round of the Rijndael Block Cipher, comprising the steps of

creating a look-up table for the multiplicative inverse in the finite field $GF(2^8)$;

providing an affine-all transformation consisting of an affine and inverse affine transformation in a single affine transformation, using the equations:

$$b'_0=[(b_0 \cdot p_0)\oplus(b_1 \cdot p_1)\oplus(b_2 \cdot p_2)\oplus(b_3 \cdot p_3)\oplus(b_4 \cdot p_4)\oplus(b_5 \cdot p_5)\oplus(b_6 \cdot p_6)\oplus(b_7 \cdot p_7)]\oplus v_0$$
$$b'_1=[(b_0 \cdot p_7)\oplus(b_1 \cdot p_0)\oplus(b_2 \cdot p_1)\oplus(b_3 \cdot p_2)\oplus(b_4 \cdot p_3)\oplus(b_5 \cdot p_4)\oplus(b_6 \cdot p_5)\oplus(b_7 \cdot p_6)]\oplus v_1$$
$$b'_2=[(b_0 \cdot p_6)\oplus(b_1 \cdot p_7)\oplus(b_2 \cdot p_0)\oplus(b_3 \cdot p_1)\oplus(b_4 \cdot p_2)\oplus(b_5 \cdot p_3)\oplus(b_6 \cdot p_4)\oplus(b_7 \cdot p_5)]\oplus v_2$$
$$b'_3=[(b_0 \cdot p_5)\oplus(b_1 \cdot p_6)\oplus(b_2 \cdot p_7)\oplus(b_3 \cdot p_0)\oplus(b_4 \cdot p_1)\oplus(b_5 \cdot p_2)\oplus(b_6 \cdot p_3)\oplus(b_7 \cdot p_4)]\oplus v_3$$
$$b'_4=[(b_0 \cdot p_4)\oplus(b_1 \cdot p_5)\oplus(b_2 \cdot p_6)\oplus(b_3 \cdot p_7)\oplus(b_4 \cdot p_0)\oplus(b_5 \cdot p_1)\oplus(b_6 \cdot p_2)\oplus(b_7 \cdot p_3)]\oplus v_4$$
$$b'_5=[(b_0 \cdot p_3)\oplus(b_1 \cdot p_4)\oplus(b_2 \cdot p_5)\oplus(b_3 \cdot p_6)\oplus(b_4 \cdot p_7)\oplus(b_5 \cdot p_0)\oplus(b_6 \cdot p_1)\oplus(b_7 \cdot p_2)]\oplus v_5$$
$$b'_6=[(b_0 \cdot p_2)\oplus(b_1 \cdot p_3)\oplus(b_2 \cdot p_4)\oplus(b_3 \cdot p_5)\oplus(b_4 \cdot p_6)\oplus(b_5 \cdot p_7)\oplus(b_6 \cdot p_0)\oplus(b_7 \cdot p_1)]\oplus v_6$$
$$b'_7=[(b_0 \cdot p_1)\oplus(b_1 \cdot p_2)\oplus(b_2 \cdot p_3)\oplus(b_3 \cdot p_4)\oplus(b_4 \cdot p_5)\oplus(b_5 \cdot p_6)\oplus(b_6 \cdot p_7)\oplus(b_7 \cdot p_0)]\oplus v_7$$

---

having $p = p_0p_1p_2p_3p_4p_5p_6p_7$ as a load pattern consisting of {10001111} for the affine transformation and {00100101} for the inverse affine transformation and having v as a load vector = $v_0v_1v_2v_3v_4v_5v_6v_7$ consisting of {11000110} for the affine transformation and {10100000} for the inverse affine transformation;

composing an S-box constructed of the look-up table and the affine-all transformation; and

performing a non-linear byte substitution using the composed S-box.

15. (Previously presented) The method of claim 14, wherein the providing step further comprises the step of providing a shared logic circuit that performs the single affine transformation.

16. (Previously presented) The method of claim 14, further comprising the step of storing the look-up table in a read-only memory (ROM).

17. (Previously presented) The method of claim 16, wherein the providing step further comprises the step of implementing a shared logic circuit that performs the single affine transformation.

18. (Previously presented) The method of claim 14, wherein:

the look-up table is the multiplicative inverse in the finite field GF(2^8) having {00} mapped to itself; and

the providing step further comprises the step of implementing a combinational logic circuit that performs the single affine transformation.

19. (Previously presented) The apparatus as claimed in claim 4, wherein, for a given input vector having a number of bits, the shared logic is configured to perform an inverse affine transform responsive to one load pattern and to perform an affine transformation responsive to another load pattern, the load patterns having the same number of bits as the input vector.